Privacidade no email

Fevereiro de 2009

Luís Morais

1 Introdução

Desde a génese da Internet e, principalmente, com a sua massificação, o correio electrónico é um dos instrumentos mais usado no dia-a-dia dos internautas e das empresas. Para este sucesso muito contribuem a facilidade de utilização, a velocidade e reduzido custo de operação e a universalidade do acesso. No entanto, a segurança deste serviço, no que diz respeito à integridade e confidencialidade das mensagens, não faz parte destas características: o email, sem mecanismos adicionais, não é, nem pode ser utilizado, como um meio seguro de comunicação e transmissão de informação.

Para colmatar esta limitação, têm vindo a ser criadas e disponibilizadas um conjunto de soluções que permitem adicionar a integridade e a confidencialidade numa comunicação de correio electrónico. Este documento tem como objectivo apresentar um conjunto destas soluções disponíveis.

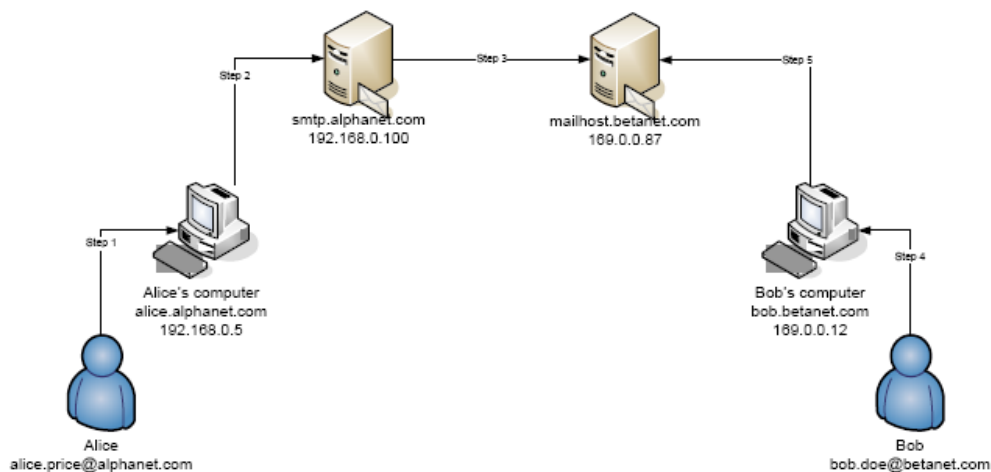
Este documento começa por descrever o processo de elaboração e transmissão de uma mensagem de correio electrónico, as suas características e fragilidades sendo de seguida apresentado um conjunto de soluções.

2 Funcionamento e fragilidades do correio electrónico

Um email começa por ser criado numa aplicação cliente (eg. MS Outlook, Thunderbird, Apple Mail) ou numa interface web (eg. Gmail, Hotmail, Outook Web Access). A operação de envio da mensagem estabelece uma ligação entre o computador pessoal e um servidor de envio de correio electrónico, conhecido como MTA (*Mail Transfer Agent*).

Este MTA remetente vai em seguida identificar o servidor MDA (*Mail Delivery Agent*) responsável por cada um dos endereços de correio electrónico identificados como destinatário da mensagem. Esta identificação recorre a bases de dados públicas configurados no serviço DNS (*Domain Name System*). Identificado(s) o(s) servidores (MDA) de destino a mensagem é então transmitida entre estes dois servidores. Esta transmissão é efectuada através do protocolo de comunicação SMTP (*Simple Mail Transfer Protocol*).

Do outro lado, novamente com recurso a uma aplicação cliente ou interface Web, o destinatário consulta regularmente o seu servidor (MDA) para obter as novas menagens. A comunicação com o servidor (MDA) é efectuada com recurso aos protocolos de comunicação POP3 (*Post Office Protocol 3*) ou IMAP (*Internet Message Access Protocol*).

Vejamos o exemplo da imagem seguinte, em que a Alice, cujo email é alice.price@alphanet.com pretende enviar um email para o Bob cujo endereço é bob.doe@betanet.com. Depois desta compor a mensagem na sua aplicação cliente (através do seu computador pessoal), a Alice procede ao seu envio.

O seu computador pessoal transmite a mensagem ao seu servidor de correio electrónico (*SMTP server* - smtp.alphanet.com). De seguida, e já sem intervenção da Alice o servidor smtp.alphanet.com verifica que o destinatário da mensagem tem como domínio betanet.com cujo servidor de correio electrónico é mailhost.betanet.com. De seguida o servidor smtp.alphanet.com estabelece uma ligação com o servidor mailhost.betanet.com através da qual envia a mensagem da Alice. Após este passo o servidor mailhost.betanet.com armazena a mensagem na *inbox* do Bob. O Bob mais tarde utiliza a sua aplicação cliente de email, que vai contactar o servidor mailhost.betanet.com utilizando o protocolo POP3 ou IMAP, e recebe finalmente a mensagem enviada pela Maria no seu computador.

Durante todo este processo são várias as vulnerabilidades a que a mensagem está exposta. Em particular, e no âmbito deste documento, a **privacidade** e a **integridade** desta pode ser comprometida:

1. Durante a utilização de uma interface web, na comunicação entre o browser do cliente e o servidor web, tanto no envio como recepção e leitura das mensagens (através do protocolo HTTP),
2. Durante a comunicação entre a aplicação cliente de email e o servidor (MTA) do remetente da mensagem (através do protocolo SMTP),
3. Durante o processamento e encaminhamento das mensagens no servidor (MTA) do remetente ou noutros servidores intermediários.
4. Durante a comunicação entre o servidor (MTA) do remetente, ou outros intermediários e o servidor (MDA) do destinatário,
5. Durante o armazenamento das mensagens no servidor (MDA) do destinatário, e
6. Durante a resolução de nomes (obtenção do servidor de correio electrónico do destinatário).

Nos pontos 1,2 e 4 a privacidade pode ser comprometida através da espionagem, intercepção e adulteração das comunicações entre servidores ou entre clientes (interfaces web ou aplicações) por terceiros. Sendo a Internet um meio de comunicação inseguro e sujeito a intercepções, as mensagens trocadas podem ser interceptadas, lidas e modificadas por utilizadores mal intencionados.

Nos pontos 2 e 5 a privacidade pode ser comprometida através da exploração de uma qualquer vulnerabilidade nesse tipo de servidores que permita, a terceiros, o acesso, leitura e alteração das mensagens armazenadas ou em trânsito. De igual modo um

administrador de sistemas mal intencionado que aproveite o acesso legítimo a um servidor (MTA ou MDA) pode espiar e modificar as mensagens lá armazenadas.

No ponto 6, através de um ataque de Pharming (para mais informações ver http://www.cert.pt/download/REC-PHARM.pdf) é possível induzir a aplicação cliente ou um servidor a entregar a mensagem a um servidor ilegítimo, controlado por utilizadores mal intencionados, ficando posteriormente a informação contida nesse email ao dispor desses mesmos utilizadores.

3 Privacidade no correio electrónico

3.1 Segurança no acesso

Por acesso entende-se a comunicação entre o computador pessoal e servidor de correio electrónico (MTA no caso do envio e MDA na recepção).

Uma solução que permite corrigir parte destas vulnerabilidades apresentadas no capítulo 1 é a utilização de mecanismos de comunicação segura entre os vários nós (aplicações cliente, interfaces web e servidores), nomeadamente os protocolos TLS (*Transport Layer Security*) e SSL (*Secure Sockets Layer*).

Ambos estes protocolos criptográficos permitem a codificação das comunicações entre os vários nós numa rede, dificultando deste modo a espionagem e adulteração das várias mensagens trocadas entre os nós, nomeadamente entre as aplicações cliente e os servidores, entre servidores e no acesso ás aplicações cliente com interfaces na web.

O utilizador deve, sempre que possível, utilizar ligações seguras ao conectar-se aos seus servidores (MTA e MDA) quando utilizar uma aplicação de email. Ao escolher ligações seguras com os seus servidores um cliente garante não só a privacidade e segurança das mensagens trocadas como também dos dados de acesso geralmente necessárias nos servidores. Informe-se junto do seu prestador de serviços de email se os respectivos servidores suportam ligações seguras e caso estas sejam suportadas configure a sua aplicação cliente de email para utilizar sempre este tipo de ligações.

Tal como na comunicação com os servidores de email, também na comunicação com as interfaces de correio electrónico na web os dados trocados circulam desprotegidos pela rede na comunicação entre o computador pessoal e o servidor web. Tente, sempre que possível, utilizar uma ligação segura na comunicação com as interfaces web. É possível verificar se está a utilizar uma ligação segura ao aceder a uma determinada interface web verificando se o endereço na barra de endereços é precedido por http:// ou http**s**://, sendo que no primeiro caso está a utilizar uma ligação não codificada e no segundo caso está a utilizar uma ligação segura.

Muitas interfaces web de correio electrónico utilizam ligações seguras apenas na autenticação, sendo que depois na leitura, composição e envio dos email utilizam apenas ligações não codificadas. Em alguns casos (ex: Gmail) é possível "forçar" a interface a utilizar ligações seguras trocando na barra de endereços o http://endereço por http**s**://endereço.

Este tipo de ligações no entanto pode não estar implementada em todos os servidores, e mesmo estando implementada para a comunicação entre um cliente e um determinado servidor, não é garantido que a comunicação entre servidores e entre o

destinatário e o seu servidor estejam igualmente protegidas, sendo sempre possível a espionagem, intercepção e adulteração da mensagem no seu percurso até ao destinatário.

3.2 Codificação e Assinatura de Mensagens

Para lidar com as vulnerabilidades descritas no capítulo 1 de uma forma mais eficaz surgiu a codificação a assinatura das mensagens de email através de mecanismos criptográficos.

Estes mecanismos permitem a codificação, através de criptografia assimétrica, de um determinada mensagem (e respectivos anexos), garantindo desta forma a **confidencialidade** da mensagem enviada já que apenas o destinatário consegue descodificar e ler a mensagem (e respectivos anexos) enviada.

Adicionalmente, e recorrendo também à criptografia assimétrica, este tipo de mecanismos permite ainda a assinatura de mensagens, garantindo assim a **autenticidade e integridade** do remetente e do conteúdo da mensagem enviado por este.

Dentro dos mecanismos de codificação de mensagens de email destacam-se dois sistemas diferentes e amplamente utilizados: O OpenPGP e o S/MIME.

Ambos os sistemas tem por base o paradigma da criptografia assimétrica, o que significa que cada utilizador tem um par de chaves criptograficas, uma privada (que deve proteger a todo o custo) e uma chave pública que divulga a todos os utilizadores com quem pretende comunicar.

Para garantir a **confidencialidade** de uma determinada mensagem o remetente de uma mensagem deve **codificar** o conteúdo desta utilizando a chave pública do destinatário. Desta forma apenas o destinatário pode descodificar, utilizando a sua chave privada, a mensagem enviada.

Para garantir **autenticidade e integridade** de uma mensagem enviada o remetente deve **assinar digitalmente** a mensagem usando a sua chave privada. A assinatura da mensagem não altera o seu conteúdo, apenas é acrescentado um valor que pode ser confirmado pelo destinatário utilizando a chave pública do remetente. Caso o valor esteja correcto é possível garantir que aquela mensagem, com aquele conteúdo, foi realmente enviada por aquele remetente.

Os dois sistemas são semelhantes no seu funcionamento, ambos funcionam ao nível do utilizador sendo este responsável por codificar ou assinar a mensagem antes de proceder ao envio para o seu MTA. A diferença principal está no mecanismo de confiança das de chaves criptográficas utilizadas.

3.2.1 S/MIME e cartão de cidadão

O S/MIME (Secure / Multipurpose Internet Mail Extensions) é uma extensão que permite a assinatura digital e codificação das mensagens de email recorrendo a certificados digitais. Estes certificados tem que ser obtidos de uma autoridade de certificação (CA – Certification Authority) válida. Uma CA válida, assina digitalmente a chave pública de um cliente, garantindo assim a autenticidade desta e criando uma

hierarquia. Essa hierarquia tem por base o padrão X.509 que define, entre outros, uma infra-estrutura de chaves públicas. A autoridade de certificação atesta que aquela chave pública é confiável e válida, podendo desta forma ser utilizada por qualquer utilizador para verificar assinaturas digitais ou para codificar mensagens.

A desvantagem deste tipo de sistemas é o custo da emissão dos certificados pelas diversas CA e reduzido prazo de validade destes certificados.

O S/MIME é suportado pela grande generalidade das aplicações de email mais utilizadas, sendo apenas necessário instalar o certificado digital depois de emitido pela respectiva CA. As aplicações de email que suportam S/MIME são:

- Microsoft Outlook/Outlook Express (Windows)
- Mozilla Thunderbird (Windows, Linux, Mac)
- Lotus Notes (Windows, Mac)
- Apple Mail (Mac)
- OpenSSL (Linux)
- Etc…

Actualmente com o **cartão do cidadão** é fornecido já com um certificado digital que permite a assinatura e codificação de emails. Para ter acesso a estes certificados basta que tenha um leitor apropriado e que siga as instruções do "*Manual de Utilização - Aplicação do Cartão de Cidadão*" que pode consultar em http://www.cartaodecidadao.pt/media/Manual_Utilizacao_Cartao_Cidadao_v121.pdf.

Para mais informações acerca desta funcionalidade consulte os serviços do cartão do cidadão em http://www.cartaodecidadao.pt .

3.2.2 OpenPGP

O OpenPGP (Open Pretty Good Privacy) é um protocolo que permite assinar, verificar integridade, codificar e descodificar criptograficamente mensagens de email, ficheiros de dados e outros. Foi definido no RFC4880 com base no PGP, um software desenvolvido por Philip Zimmermann.

O OpenPGP surgiu com o conceito "web of trust" (rede de confiança) em que em detrimento de autoridades de certificação que garantem a validade e veracidade da chave pública de um determinado utilizador, as chaves públicas seriam assinadas por outros utilizadores que garantiam que aquela chave pertence realmente àquele utilizador, e daí estabeleciam-se redes de confiança através de utilizadores confiáveis. Adicionalmente seria sempre possível obter a chave pessoalmente e adicioná-la ao circulo de confiança.

Foram também criados servidores para onde é possível fazer o upload de uma chave pública para que outros possam efectuar uma pesquisa e efectuar o download das chaves dos vários utilizadores. Este método não é no entanto totalmente fiável, sendo possível alterar as chaves públicas publicadas.

A grande vantagem deste tipo de sistemas prende-se com os custos, que em muitos casos não existem. Como não existem CA não ha necessidade de pagar valores avultados por emissão ou renovação de um certificado. Existem ainda muitas aplicações open source que implementam o OpenPGP e que não apresentam quaisquer custos para o utilizador.

Com a evolução as aplicações OpenPGP começaram também a suportar os certificados X.509 e em alguns casos S/MIME.

Existem diversas aplicações que OpenPGP para codificação e assinatura de mensagens de email. Enquanto que algumas são embutidas na aplicação cliente (enigmail+GnuPG) outras funcionam como um proxy que se situa entre a aplicação cliente e os servidores MTA e MDA (PGP Desktop), permitindo a codificação e assinatura das mensagens depois destas serem enviadas pelo cliente de email e a descodificação e verificação de assinaturas antes destas serem recebidas na aplicação.

As opções disponíveis e mais utilizadas actualmente são:

- PGP Desktop (http://www.pgp.com) – Aplicação comercial que permite a codificação e assinatura de mensagens de email e de ficheiros de dados armazenados em disco através do OpenPGP ou S/MIME. Funciona como um proxy entre as aplicações cliente suportadas (Microsoft Outlook/Outlook Express, Mozilla Thunderbird, Lotus Notes, Apple Mail, etc...) e os servidores MTA e MDA. Está numa fase estável da evolução e é suportada em Microsoft Windows 2000/2003/XP/Vista e Apple Mac OS X.

- GnuPG (http://gnupg.org/) – Implementação open source do OpenPGP. Existem versões para quase todos os sistemas operativos (Microsoft Windows, Mac OS X, Linux, BSD, Solaris, etc...). O GnuPG dispõe apenas de uma interface por linha de comandos o que o torna extremamente difícil de utilizar no dia a dia. O que levou ao surgimento de plugins e outras aplicações que utilizam o GnuPG nos mais variados sistemas operativos ou clientes de email, como por exemplo:
  - Enigmail (http://enigmail.mozdev.org/home/index.php) – Plugin open source para o cliente de email Mozilla Thunderbird (igualmente open source) que utilizando como base o GnuPG oferece possibilidade de assinatura e codificação criptográficas de mensagens embutida no Thunderbird. Encontra-se numa fase madura da sua evolução e é suportado em Microsoft Windows, Apple Mac OS X e Linux.
  - Gpg4win (http://www.gpg4win.org/) – Plugin open source para Microsoft Windows que inclui também um plugin para Microsoft Outlook 2003 e que também oferece, com base no GnuPG, a codificação e assinatura de mensagens embutida neste cliente de email. Adicionalmente permite também a codificação de ficheiros armazenados em disco. Suportado apenas em Microsoft Windows.
  - GPGMail (http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html) – Plugin open source para o Apple Mail que permite, com base no GnuPG, a codificação e assinatura de mensagens embutida neste cliente de email. Suportado em Mac OS X.

Existem bastante mais soluções disponíveis para além das acima descritas, sendo estas as mais utilizadas pelo público geral.

3.2.3 Outras formas de codificação

Existem outros métodos de codificação que não recorrem a criptografia, mas sim a palavras passe. Estes métodos são bastante menos eficazes mas é possível introduzir alguma segurança a um custo baixo e utilizando ferramentas amplamente utilizadas, como por exemplo:

- Ficheiros compactados (Zip, rar, tar, etc...) e protegidos por palavras passe,
- Ficheiros Office protegidos por palavra passe,
- Utilização de servidores de alojamento (Ftp, http, ...) seguro para alojamento temporário de informações ou documentos sensíveis com acesso compartilhado por ambos os utilizadores,
- Etc...

4 Referências

Internet Segura – Correio Electrónico
http://www.internetsegura.pt/pt-PT/Perigos/email/ContentDetail.aspx

Cuidados com correio electrónico
http://www.cert.pt/download/REC-EM.pdf

Manual de Utilização - Aplicação do Cartão de Cidadão
http://www.cartaodecidadao.pt/media/Manual_Utilizacao_Cartao_Cidadao_v121.pdf

S/MIME Version 3.1 Message Specification
http://www.ietf.org/rfc/rfc3851.txt

OpenPGP Message Format
http://tools.ietf.org/html/rfc4880

Internet X.509 Public Key Infrastructure
www.ietf.org/rfc/rfc2459.txt

E-mail client testing for S/MIME compliance
http://www.ripe.net/db/support/security/mail_client_tests.html

InternetSegura.PT
http://www.internetsegura.pt

CERT.PT
http://www.cert.pt